On the large sieve with sparse sets of moduli

Stephan Baier

22.08.05

Address of the author:

Stephan Baier
Jeffery Hall
Department of Mathematics and Statistics
Queen's University
University Ave
Kingston, Ontario, Canada
K7L 3N6

e-mail: sbaier@mast.queensu.ca

Abstract: Extending a method of D. Wolke [10], we establish a general result on the large sieve with sparse sets $\mathcal{S}$ of moduli which are in a sense well-distributed in arithmetic progressions. We then use this result together with Fourier techniques to obtain large sieve bounds for the case when $\mathcal{S}$ consists of sqares. These bounds improve a recent result by L. Zhao [11].

Mathematics Subject Classification (2000): 11N35, 11L07, 11B57

Key words: large sieve, Farey fractions in short intervals, estimates on exponential sums

1 A general result on the large sieve

Throughout this paper, we reserve the symbols c_i $(i = 1, 2, ...)$ for absolute constants and the symbol ε for an arbitrary (small) positive number. The $\ll$-constants in our estimates may depend on ε. As usual in analytic number theory, the ε may be different from line to line. We further suppose that (a_n) is a sequence of complex numbers and that $Q, N \geq 1$. We set

$$S(\alpha) := \sum_{n \leq N} a_n e(n\alpha). \tag{1}$$

Bombieri's [3] classical large sieve inequality asserts that

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \leq (N + Q^2)Z, \tag{2}$$

where

$$Z := \sum_{n \leq N} |a_n|^2.$$

One may ask whether (2) can be improved if the moduli q run over a sparse set $\mathcal{S}$ of natural numbers $\leq Q$. It seems to be difficult to obtain a considerable improvement if nothing is known about the structure of $\mathcal{S}$. The goal of the present paper is to improve (2) for sets $\mathcal{S}$ of moduli which are in a sense well-distributed in arithmetic progressions.

In the sequel, we suppose, more generally, that $\mathcal{S} \subset (M, M+Q]$, where $0 \le M \le Q$. We put $S := |\mathcal{S}|$ (the cardinality of $\mathcal{S}$). For $t \in \mathbb{N}$ we put

$$\mathcal{S}_t := \{q \in \mathbb{N} \ : \ tq \in \mathcal{S}\}$$

and $S_t := |\mathcal{S}_t|$. We note that $\mathcal{S}_t \subset (M/t, M/t + Q/t]$. We shall require that the number of elements of $\mathcal{S}_t$ in short segments of arithmetic progressions does not differ too much from the expected number. To measure the distribution of $\mathcal{S}_t$ in segments of arithmetic progressions, we define the quantity

$$A_t(u,k,l) := \max_{M/t \le y \le (M+Q)/t} |\{q \in \mathcal{S}_t \cap (y, y+u] \ : \ q \equiv l \bmod k\}|,$$

where $u \ge 0$, $k \in \mathbb{N}$, $l \in \mathbb{Z}$ with $(k,l) = 1$. We shall establish the following

Theorem 1: *We have*

$$\sum_{q \in \mathcal{S}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right)\right|^2 \ \le \ c_1 NZ \left(1 + \max_{r \le \sqrt{N}} \max_{1/N \le z \le 1/(r\sqrt{N})} \max_{\substack{h \in \mathbb{Z} \\ (h,r)=1}} \sum_{t|r} \sum_{\substack{0 < |m| \le 6rzQ/t \\ (m, r/t) = 1}} A_t\left(\frac{2Q}{tzN}, \frac{r}{t}, hm\right)\right).$$

If we assume the set $\mathcal{S}_t$ to be nearly evenly distributed in the residue classes $l \bmod k$, then, if $M/t \le y \le (M+Q)/t - u$, the expected number of elements of the set

$$\{q \in \mathcal{S}_t \cap (y, y+u] \ : \ q \equiv l \bmod k\}$$

is

$$\frac{S_t/k}{Q/t} \cdot u.$$

Therefore, if $\mathcal{S}_t$ is well-distributed in the residue classes $l \bmod k$, we may expect, for any $u \ge 0$, that

$$A_t(u,k,l) \le \left(1 + \frac{S_t/k}{Q/t} \cdot u\right) X, \tag{3}$$

where $X \geq 1$ is small compared to Q and N.

By a short calculation, we infer the following bound from Theorem 1.

Theorem 2: *Suppose the condition (3) to hold for all t, k, l, u with $t \leq \sqrt{N}$, $k \leq \sqrt{N}/t$, $(k,l) = 1$ and $kQ/\sqrt{N} \leq u \leq Q/t$. Then*

$$\sum_{q \in \mathcal{S}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \leq c_2 \left(N + QXN^{\varepsilon}\left(\sqrt{N} + S\right)\right) Z. \tag{4}$$

This is stronger than the classical large sieve inequality (2) if $N^{1+\varepsilon} \ll QX(\sqrt{N} + S) \ll Q^{2-\varepsilon}$. If the set $\mathcal{S}$ is really sparse, that is, if S is small compared to Q, and if the condition (3) holds with $X = N^{\varepsilon}$, then (4) is sharper than (2) if $Q \gg N^{1/2+\varepsilon}$. In section 6 we shall see that in the case of square moduli $X = N^{\varepsilon}$ is an admissible choice in (3).

A conjecture of Elliott [5] would imply that the left-hand side of (4) is bounded by

$$\ll (N + QS)Z \tag{5}$$

if $\mathcal{S}$ contains only primes. From (4), we obtain the slightly weaker bound $\ll (N + QN^{\varepsilon}S)Z$ if $X = N^{\varepsilon}$ is admissible and $S \gg \sqrt{N}$.

2 The case of squares

Recently, L. Zhao [11] studied the case when the moduli q are squares, that is, he investigated the order of magnitude of the expression

$$T := \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right) \right|^2.$$

He proved the estimate

$$T \ll (\log 2Q) \left(Q^3 + (N\sqrt{Q} + \sqrt{N}Q^2)N^{\varepsilon}\right) Z \tag{6}$$

and conjectured that

$$T \ll Q^{\varepsilon}(Q^3 + N)Z. \tag{7}$$

The classical form (2) of the large sieve implies only the bound

$$T \ll (N + Q^4)Z, \tag{8}$$

which is weaker than (6) if $Q \gg N^{2/7+\varepsilon}$. Using the bound

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right) \right|^2 \ll (N + q^2)Z, \tag{9}$$

which follows from our later Lemma 1 with $\Delta = 1/q^2$ and (α_r) beeing the sequence formed by all fractions a/q^2 with $1 \le a \le q^2$ and $(a, q) = 1$, we also obtain the bound

$$T \ll Q(N + Q^2)Z \tag{10}$$

by summing up (9) over all $q \le Q$. This bound is weaker than (6) if $Q \ll N^{1/2-\varepsilon}$. Thus, (6) is sharper than both (8) and (10) if $N^{2/7+\varepsilon} \ll Q \ll N^{1/2-\varepsilon}$.

Employing Theorem 2 with $\mathcal{S}$ a set of squares, we shall obtain the following improvement of Zhao's bound (6).

Theorem 3: *We have*

$$T \ll (\log 2Q)N^{\varepsilon}(Q^3 + N + N^{1/2}Q^2)Z. \tag{11}$$

The bound (11) is sharper than the three bounds (6), (8) and (10) if $N^{1/4+\varepsilon} \ll Q \ll N^{1/3-\varepsilon}$. Combining the elementary methods which we will use for the proof of Theorem 3 with Fourier analytic techniques, we shall further prove

Theorem 4: *We have*

$$T \ll \begin{cases} Q^{3/5+\varepsilon}NZ, & \text{if } Q \le N^{5/12}, \\ Q^{3+\varepsilon}Z, & \text{if } Q > N^{5/12}. \end{cases}$$

This bound is sharper than (6), (8) and (10) if $N^{5/14+\varepsilon} \ll Q \ll N^{1/2-\varepsilon}$. Moreover, it establishes Zhao's conjecture (7) for $Q \gg N^{5/12}$.

3 The case of primes

For the case when $\mathcal{S}$ is the full set of all primes $p \le Q$ D. Wolke [10] proved the estimate

$$\sum_{p\le Q}\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}\right)\right|^2 \le \frac{c_3}{1-\delta}\frac{Q^2\log\log Q}{\log Q}Z \tag{12}$$

provided that

$$Q \ge 10, \qquad N = Q^{1+\delta}, \qquad 0 < \delta < 1. \tag{13}$$

In this range Elliott's conjecture (5) would give the slightly better bound $\ll Q^2 Z/\log Q$.

Now we want to prove that Theorem 1 with $M = 0$ and $\mathcal{S}$ beeing the set of all primes $p \le Q$ implies Wolke's bound (12). We need to estimate the term $A_t(u,k,l)$. First we consider the case when $t = 1$. By the Brun-Titchmarsh inequality, we have

$$A_1\left(\frac{2Q}{zN}, r, l\right) \le \frac{4Q}{zN\varphi(r)\log(2Q/rzN)} \tag{14}$$

if $2Q/(zN) > r$. If $rz \le 1/\sqrt{N}$, then $2Q/(zN) > r$ is satisfied since $1/\sqrt{N} < 2Q/N$ by (13). From (13) and (14), we deduce

$$\sum_{\substack{0<|m|\le 6rzQ\\(m,r)=1}} A_1\left(\frac{2Q}{zN}, r, hm\right) \le c_4\frac{Q^2\log\log Q}{N(1-\delta)\log Q} \tag{15}$$

for any integer h with $(r,h) = 1$.

If $t \ge 2$, then $\mathcal{S}_t$ contains at most 1 element. This implies

$$\begin{aligned}\sum_{\substack{t|r\\t\ge 2}}\sum_{\substack{0<|m|\le 6rzQ/t\\(m,r/t)=1}} A_t\left(\frac{2Q}{tzN}, \frac{r}{t}, hm\right)\\ \le \sum_{t|r}\frac{12rzQ}{t} \le c_5 rzQ\log\log 10r \le c_6\frac{Q\log\log Q}{\sqrt{N}}\end{aligned} \tag{16}$$

if $r \leq \sqrt{N} < Q$ and $z \leq 1/(r\sqrt{N})$. Using $N = Q^{1+\delta}$, it is easy to check that there exists a constant c_7 such that we have

$$\frac{Q \log\log Q}{\sqrt{N}} \leq c_7 \frac{Q^2 \log\log Q}{N(1-\delta)\log Q} \tag{17}$$

for all $Q \geq 10$ and $0 < \delta < 1$. From Theorem 1, (15), (16) and (17), we obtain Wolke's bound (12).

4 Counting Farey fractions in short intervals

In this section we establish some preliminary results which we then use for the proof of Theorem 1. Our starting point is the following variant of the large sieve which follows immediately from Theorem 2.11 in [7].

Lemma 1: *Let $(\alpha_r)_{r\in\mathbb{N}}$ be a sequence of real numbers. Suppose that $0 < \Delta \leq 1/2$ and $R \in \mathbb{N}$. Put*

$$K(\Delta) := \max_{\alpha\in\mathbb{R}} \sum_{\substack{r=1 \\ ||\alpha_r - \alpha|| \leq \Delta}}^{R} 1,$$

where $||x||$ denotes the distance of a real x to its closest integer. Then

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq c_8 K(\Delta)(N + \Delta^{-1})Z.$$

In our situation, the sequence $\alpha_1, ..., \alpha_R$ equals the sequence of Farey fractions a/q with $q \in \mathcal{S}$, $1 \leq a \leq q$ and $(a,q) = 1$. For $\alpha \in \mathbb{R}$ we put

$$I(\alpha) := [\alpha - \Delta, \alpha + \Delta] \quad \text{and} \quad P(\alpha) := \sum_{\substack{q\in\mathcal{S},(a,q)=1 \\ a/q \in I(\alpha)}} 1.$$

Then we have

$$K(\Delta) = \max_{\alpha\in\mathbb{R}} P(\alpha). \tag{18}$$

To estimate $P(\alpha)$, we begin with a method of D. Wolke [10]. Let

$$\tau := \frac{1}{\sqrt{\Delta}}. \tag{19}$$

Then, by Dirichlet's approximation theorem, α can be written in the form

$$\alpha = \frac{b}{r} + z, \quad \text{where} \quad r \le \tau,\ (b,r) = 1,\ |z| \le \frac{1}{r\tau}. \tag{20}$$

Thus, it suffices to estimate $P(b/r + z)$ for all b, r, z satisfying (20).

We further note that we can restrict ourselves to the case when

$$z \ge \Delta. \tag{21}$$

If $|z| < \Delta$, then

$$P(\alpha) \le P\left(\frac{b}{r} - \Delta\right) + P\left(\frac{b}{r} + \Delta\right).$$

Furthermore, we have

$$\Delta = \frac{1}{\tau^2} \le \frac{1}{r\tau}.$$

Therefore this case can be reduced to the case $|z| = \Delta$. Moreover, as $P(\alpha) = P(-\alpha)$, we can choose z positive. So we can assume (21).

Summarizing the above observations, we deduce

Lemma 2: *We have*

$$K(\Delta) \le 2 \max_{\substack{r \in \mathbb{N} \\ r \le 1/\sqrt{\Delta}}} \max_{\substack{b \in \mathbb{Z} \\ (b,r)=1}} \max_{\Delta \le z \le \sqrt{\Delta}/r} P\left(\frac{b}{r} + z\right). \tag{22}$$

The next lemma provides a first estimate for $P\left(b/r + z\right)$.

Lemma 3: *Suppose that the conditions (19), (20) and (21) are satisfied. Suppose further that*

$$\frac{Q\Delta}{z} \le \delta \le Q. \tag{23}$$

Let $I(\delta, y) := [y-\delta, y+\delta]$, $J(\delta, y) := [(y-4\delta)rz, (y+4\delta)rz]$ *and*

$$\Pi(\delta, y) := \sum_{q \in \mathcal{S} \cap I(\delta, y)} \sum_{\substack{m \in J(\delta, y) \\ m \equiv -bq \bmod r \\ m \neq 0}} 1.$$

Then,

$$P\left(\frac{b}{r} + z\right) \leq 2 + \frac{1}{\delta} \int_{M}^{M+Q} \Pi(\delta, y) \, \mathrm{d}y.$$

Proof: By $\delta \leq Q$, we have

$$P(\alpha) \leq \frac{1}{\delta} \int_{M}^{M+Q} P(\alpha, y, \delta) \, \mathrm{d}y, \tag{24}$$

where

$$P(\alpha, y, \delta) := \sum_{\substack{q \in \mathcal{S} \cap I(\delta, y) \\ (a, q) = 1 \\ a/q \in I(\alpha)}} 1.$$

Now, for $a/q \in I(\alpha)$, we have

$$q(\alpha - \Delta) \leq a \leq q(\alpha + \Delta).$$

From this and $\alpha = b/r + z$, we obtain

$$qr(z - \Delta) \leq ar - bq \leq qr(z + \Delta). \tag{25}$$

If $y - \delta \leq q \leq y + \delta$, then from (20), (21), (23) and (25) it follows that

$$(y-4\delta)rz \leq (y-\delta)r(z-\Delta) \leq ar-bq \leq (y+\delta)r(z+\Delta) \leq (y+4\delta)rz. \tag{26}$$

If $ar - bq = 0$, then $r = q$ because $(a, q) = 1 = (b, r)$. From this observation, (24) and (26), we deduce the result of Lemma 3.□

5 Proof of Theorem 1

Next, we express $\Pi(y,\delta)$ in terms of $A_t(u,k,l)$. This shall lead us to the following estimate for $P(b/r+z)$.

Lemma 4: *We have*

$$P\left(\frac{b}{r}+z\right) \le 2 + c_9 \sum_{t|r} \sum_{\substack{0<|m|\le 6rzQ/t \\ (m,r/t)=1}} A_t\left(\frac{2\Delta Q}{tz}, \frac{r}{t}, -\overline{b}m\right),$$

where $\overline{b}b \equiv 1 \ mod\ r$.

On choosing $\Delta := 1/N$, Theorem 1 follows immediately from Lemmas 1,2 and 4.

Proof of Lemma 4: We split $\Pi(\delta,y)$ into

$$\Pi(\delta,y) = \sum_{t|r} \sum_{\substack{q\in\mathcal{S}_t\cap I(\delta/t,y/t) \\ (q,r/t)=1}} \sum_{\substack{m\in J(\delta/t,y/t) \\ m\equiv -bq \bmod r/t \\ m\neq 0}} 1.$$

Rearranging the order of summation, and using the definition of $A_t(u,k,l)$, the right-hand side is

$$\begin{aligned} (27) \qquad &= \sum_{t|r} \sum_{\substack{m\in J(\delta/t,y/t) \\ (m,r/t)=1 \\ m\neq 0}} \sum_{\substack{q\in\mathcal{S}_t\cap I(\delta/t,y/t) \\ q\equiv -\overline{b}m \bmod r/t}} 1 \\ &\le \sum_{t|r} \sum_{\substack{m\in J(\delta/t,y/t) \\ (m,r/t)=1 \\ m\neq 0}} A_t\left(\frac{2\delta}{t}, \frac{r}{t}, -\overline{b}m\right). \end{aligned}$$

Integrating the last line of (27) over y in the interval $M \le y \le M+Q$, and

rearranging the order of summation and integration, we obtain

(28)
$$\int_M^{M+Q} \Pi(\delta, y)\ \mathrm{d}y \le 2\delta \sum_{t|r} \sum_{\substack{(M-4\delta)rz/t \le m \le (M+Q+4\delta)rz/t \\ (m, r/t) = 1 \\ m \ne 0}} A_t\left(\frac{2\delta}{t}, \frac{r}{t}, -\overline{b}m\right).$$

Choosing $\delta := Q\Delta/z$, and taking $0 \le M \le Q$ and $Q\Delta/z \le Q$ into account, we obtain the result of Lemma 4 from Lemma 3 and (28). □

From Lemma 4, we also infer the following estimate for $P(b/r + z)$ by a short calculation.

Lemma 5: *Suppose that the conditions (19), (20) and (21) are satisfied. Suppose further the condition (3) to hold for $t|r$, $k = r/t$, $(k, l) = 1$ and $u = 2\Delta Q/(tz)$. Then*

$$P\left(\frac{b}{r} + z\right) \le c_{10}\left(1 + QX\Delta^{-\varepsilon}\left(rz + \Delta S\right)\right) Z.$$

This estimate corresponds to Theorem 2. We shall use it in section 7.

6 Proof of Theorem 3

In this section, we derive Theorem 3 from Theorem 2. First, we rewrite the sum in question in the form

$$T = \sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left|S\left(\frac{a}{q^2}\right)\right|^2 = \sum_{q \in \mathcal{S}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2,$$

where $\mathcal{S}$ is the set of squares $\le Q^2$. We split up the set $\mathcal{S}$ into $O(\log Q)$ subsets of the form

$$\mathcal{S}(Q_0) := \mathcal{S} \cap (Q_0, 2Q_0],$$

where $Q_0 \geq 1$. Our aim is to estimate the corresponding partial sums. As previously, we define

$$\mathcal{S}_t(Q_0) := \{q \in \mathbb{N} \ : \ tq \in \mathcal{S}(Q_0)\}$$

and $S_t(Q_0) := |\mathcal{S}_t(Q_0)|$. We now determine the set $\mathcal{S}_t(Q_0)$. Let $t = p_1^{v_1} \cdots p_n^{v_n}$ be the prime number factorization of t. For $i = 1, ..., n$ let

$$u_i := \begin{cases} v_i, & \text{if } v_i \text{ is even,} \\ \\ v_i + 1, & \text{if } v_i \text{ is odd.} \end{cases}$$

Put

$$f_t := p_1^{u_1/2} \cdots p_n^{u_n/2}.$$

Then $q = q_1^2 \in \mathcal{S}$ is divisible by t iff q_1 is divisible by f_t. Thus,

$$\mathcal{S}_t(Q_0) = \left\{q_2^2 g_t \ : \ \sqrt{Q_0}/f_t < q_2 \leq \sqrt{2Q_0}/f_t\right\} \subset (Q_0/t, 2Q_0/t],$$

where

$$g_t := \frac{f_t^2}{t} = p_1^{u_1 - v_1} \cdots p_n^{u_n - v_n}.$$

As previously, we suppose that $u \geq 0$, $k \in \mathbb{N}$, $l \in \mathbb{Z}$ and $(k, l) = 1$, and define

$$A_t(u, k, l) := \max_{Q_0/t \leq y \leq 2Q_0/t} |\{q \in \mathcal{S}_t(Q_0) \cap (y, y + u] \ : \ q \equiv l \bmod k\}|.$$

Let $\delta_t(k, l)$ be the number of solutions $x \bmod k$ to the congruence

$$x^2 g_t \equiv l \bmod k. \tag{29}$$

Then, from our above observations it follows quickly that

$$A_t(u, k, l) \leq c_{11} \left(1 + \frac{S_t/k}{Q/t} \cdot u\right) \delta_t(k, l).$$

The remaining task is to bound $\delta_t(k, l)$.

If $(g_t, k) > 1$, then $\delta_t(k, l) = 0$ since k and l are supposed to be coprime. Therefore, we can assume that $(g_t, k) = 1$. Let $g \bmod k$ be the multiplicative

inverse of g_t mod k, i.e. $gg_t \equiv 1 \bmod k$. Put $l^* = gl$. Then (29) is equivalent to

$$x^2 \equiv l^* \bmod k. \tag{30}$$

Taking into account that $(k, l^*) = 1$, and using some elementary facts on the number of solutions of polynomial congruences modulo prime powers (see [9], for example), we see that (30) has at most 2 solutions if k is a power of an odd prime and at most 4 solutions if k is a power of 2. From this it follows that for all $k \in \mathbb{N}$ we have

$$\delta_t(k, l) \le 2^{\omega(k)+1},$$

where $\omega(k)$ is the number of distinct prime divisors of k. For $k \le \sqrt{N}$ we have

$$2^{\omega(k)} \ll N^{\varepsilon}$$

(see [4]). Therefore, (3) holds with

$$X := c_{12} N^{\varepsilon}. \tag{31}$$

Now, from Theorem 2, (31) and $S \ll \sqrt{Q_0}$, we obtain

$$\sum_{q \in \mathcal{S}(Q_0)} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \le c_{13} \left(N + Q_0 N^{\varepsilon} \left(\sqrt{N} + \sqrt{Q_0} \right) \right) Z.$$

This implies the result of Theorem 3. □

7 Proof of Theorem 4

Throughout this section, we suppose that $\mathcal{S}$ consists of all squares in the interval $(Q_0, 2Q_0]$. To prove Theorem 4, we use the following estimates for $P(b/r + z)$.

Lemma 6: *Suppose that the conditions (19), (20) and (21) are satisfied. Then we have*

$$P\left(\frac{b}{r} + z\right) \le c_{14} \Delta^{-\varepsilon} \left(1 + Q_0 r z + Q_0^{3/2} \Delta \right) \tag{32}$$

and

$$P\left(\frac{b}{r}+z\right) \le c_{15}\Delta^{-\varepsilon}\left(Q_0^{3/2}\Delta + Q_0^{1/2}\Delta r^{-1/2}z^{-1} + \Delta^{-1/4}\right). \tag{33}$$

The inequality (32) follows immediately from Lemma 5 and the fact that (3) holds with $X := c_{16}\Delta^{-\varepsilon}$ under the conditions of Lemma 5. This can be seen in the same way as it was proved that (31) is an admissable choice in (3) under the conditions of Theorem 3.

We postpone the proof of (33) to the last section.

We are now ready to prove Theorem 4. Combining (32) and (33), we obtain

$$P\left(\frac{b}{r}+z\right) \le c_{17}\Delta^{-\varepsilon}\left(Q_0^{3/2}\Delta + \min\left\{Q_0 rz, Q_0^{1/2}\Delta r^{-1/2}z^{-1}\right\} + \Delta^{-1/4}\right). \tag{34}$$

If

$$z \le \Delta^{1/2}Q_0^{-1/4}r^{-3/4},$$

then

$$\min\left\{Q_0 rz, Q_0^{1/2}\Delta r^{-1/2}z^{-1}\right\} = Q_0 rz \le Q_0^{3/4}\Delta^{1/2}r^{1/4}.$$

If

$$z > \Delta^{1/2}Q_0^{-1/4}r^{-3/4},$$

then

$$\min\left\{Q_0 rz, Q_0^{1/2}\Delta r^{-1/2}z^{-1}\right\} = Q_0^{1/2}\Delta r^{-1/2}z^{-1} \le Q_0^{3/4}\Delta^{1/2}r^{1/4}.$$

From the above inequalities and (20), we deduce that

$$\min\left\{Q_0 rz, Q_0^{1/2}\Delta r^{-1/2}z^{-1}\right\} \le Q_0^{3/4}\Delta^{3/8}. \tag{35}$$

Furthermore,

$$Q_0^{3/4}\Delta^{3/8} = \sqrt{(Q_0^{3/2}\Delta)\cdot\Delta^{-1/4}} \le Q_0^{3/2}\Delta + \Delta^{-1/4}. \tag{36}$$

Combining (34), (35) and (36), we get

$$P\left(\frac{b}{r}+z\right) \le c_{18}\Delta^{-\varepsilon}\left(Q_0^{3/2}\Delta + \Delta^{-1/4}\right). \tag{37}$$

Now we choose

$$\Delta := \begin{cases} Q_0^{-6/5}, & \text{if } Q_0 \le N^{5/6}, \\ \\ N^{-1}, & \text{otherwise.} \end{cases}$$

Then from Lemma 1, Lemma 2 and (37) it follows that

$$\sum_{\sqrt{Q_0} \le q \le \sqrt{2Q_0}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right) \right|^2 \ll \begin{cases} Q_0^{3/10+\varepsilon} NZ, & \text{if } Q_0 \le N^{5/6}, \\ \\ Q_0^{3/2+\varepsilon} Z, & \text{otherwise.} \end{cases} \tag{38}$$

We can devide the interval $[1, Q]$ into $O(\log Q)$ subintervals of the form $\left[\sqrt{Q_0}, \sqrt{2Q_0}\right]$, where $1 \le Q_0 \le Q^2$. Hence, the result of Theorem 4 follows from (38). $\square$

8 Tools from harmonic analysis

For the proof of (33) we need the following standard results from harmonic analysis.

Lemma 7: (Poisson summation formula, [2]) *Let $f(X)$ be a complex-valued function on the real numbers that is piecewise continuous with only finitely many discontinuities and for all real numbers a satisfies*

$$f(a) = \frac{1}{2}\left(\lim_{x \to a^-} f(x) + \lim_{x \to a^+} f(x)\right).$$

Moreover, suppose that $f(x) \le c_{19}(1 + |x|)^{-c}$ for some $c > 1$. Then,

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n),$$

where

$$\hat{f}(x) := \int_{-\infty}^{\infty} f(y) e(xy) \mathrm{d}y,$$

the Fourier transform of $f(x)$.

Lemma 8: (see [11], for example) *For $x \in \mathbb{R} \setminus \{0\}$ define*

$$\phi(x) := \left(\frac{\sin \pi x}{2x}\right)^2.$$

Set

$$\phi(0) := \lim_{x \to 0} \phi(x) = \frac{\pi^2}{4}.$$

Then $\phi(x) \geq 1$ for $|x| \leq 1/2$, and the Fourier transform of the function $\phi(x)$ is

$$\hat{\phi}(s) = \frac{\pi^2}{4} \max\{1 - |s|, 0\}.$$

Lemma 9: (see Lemma 3.1. in [6]) *Let $F : [a, b] \to \mathbb{R}$ be twice differentiable. Assume that $|F'(x)| \geq u > 0$ for all $x \in [a, b]$. Then,*

$$\left| \int_a^b e^{iF(x)} \mathrm{d}x \right| \ll \frac{c_{20}}{u}.$$

Lemma 10: (see Lemma 4.3.1. in [1]) *Let $F : [a, b] \to \mathbb{R}$ be twice continuously differentiable. Assume that $|F''(x)| \geq u > 0$ for all $x \in [a, b]$. Then,*

$$\left| \int_a^b e^{iF(x)} \mathrm{d}x \right| \leq \frac{c_{21}}{\sqrt{u}}.$$

We shall also need the following estimate for quadratic Gauß sums.

Lemma 11: (see page 93 in [6]) *Let $c \in \mathbb{N}$, $k, l \in \mathbb{Z}$ with $(k, c) = 1$. Then,*

$$\sum_{d=1}^{r} e\left(\frac{kd^2 + ld}{c}\right) \leq \sqrt{2c}.$$

9 Proof of (33)

Applying Lemma 3 with Q replaced by Q_0, $M = Q_0$ and $S := \{q^2 \ : \ \sqrt{Q_0} < q \le \sqrt{2Q_0}\}$, we have, for any δ satisfying the condition (23),

$$P\left(\frac{b}{r} + z\right) \le 2 + \frac{1}{\delta} \int_{Q_0}^{2Q_0} \Pi(\delta, y)\ \mathrm{d}y, \tag{39}$$

where

$$\Pi(\delta, y) := \sum_{\sqrt{y-\delta} \le q \le \sqrt{y+\delta}} \ \sum_{\substack{m \in J(\delta, y) \\ m \equiv -bq^2 \bmod r \\ m \ne 0}} 1.$$

By Taylors formula and $\delta \le Q_0$, we have

$$\sqrt{y} - c_{22}\delta/\sqrt{Q_0} \le \sqrt{y-\delta} < \sqrt{y+\delta} \le \sqrt{y} + c_{22}\delta/\sqrt{Q_0}.$$

Hence,

$$\Pi(\delta, y) < \sum_{\sqrt{y} - c_{22}\delta/\sqrt{Q_0} \le q \le \sqrt{y} + c_{22}\delta/\sqrt{Q_0}} \ \sum_{\substack{(y-4\delta)rz \le m \le (y+4\delta)rz \\ m \equiv -bq^2 \bmod r}} 1. \tag{40}$$

By Lemma 8, the double sum on the right-hand side is bounded by

$$\le c_{23} \sum_{q \in \mathbb{Z}} \phi\left(\frac{q - \sqrt{y}}{2c_{22}\delta/\sqrt{Q_0}}\right) \sum_{\substack{m \in \mathbb{Z} \\ m \equiv -bq^2 \bmod r}} \phi\left(\frac{m - yrz}{8\delta rz}\right) \mathrm{d}y. \tag{41}$$

Using Lemma 7 after a linear change of variables, we transform the inner sum into

$$\sum_{\substack{m \in Z \\ m \equiv -bq^2 \bmod r}} \phi\left(\frac{m - yrz}{8\delta rz}\right) = 8\delta z \sum_{j \in \mathbb{Z}} e\left(\frac{jbq^2}{r} + jyz\right) \hat{\phi}(8j\delta z).$$

Therefore, the double sum in (41) is

$$= 8\delta z \sum_{j \in \mathbb{Z}} e(jyz) \hat{\phi}(8j\delta z) \sum_{d=1}^{r^*} e\left(\frac{j^* b d^2}{r^*}\right) \sum_{\substack{k \in \mathbb{Z} \\ k \equiv d \bmod r^*}} \phi\left(\frac{k - \sqrt{y}}{2c_{22}\delta/\sqrt{Q_0}}\right), \tag{42}$$

where $r^* := r/(r,j)$ and $j^* := j/(r,j)$. Again using Lemma 7 after a linear change of variables, we transform the inner sum in (42) into

(43)
$$\sum_{\substack{k \in \mathbb{Z} \\ k \equiv d \bmod r^*}} \phi\left(\frac{k-\sqrt{y}}{2c_{22}\delta/\sqrt{Q_0}}\right) = \frac{2c_{22}\delta}{r^*\sqrt{Q_0}} \sum_{l\in\mathbb{Z}} e\left(l\cdot\frac{d-\sqrt{y}}{r^*}\right)\hat{\phi}\left(\frac{2c_{22}l\delta}{r^*\sqrt{Q_0}}\right).$$

From (42) and (43), we obtain

$$\begin{aligned}(44)\quad &\frac{1}{\delta}\int_{Q_0}^{2Q_0} \sum_{q\in\mathbb{Z}} \phi\left(\frac{q-\sqrt{y}}{2c_{22}\delta/\sqrt{Q_0}}\right) \sum_{\substack{m\in\mathbb{Z}\\ m\equiv -bq^2 \bmod r}} \phi\left(\frac{m-yrz}{8\delta rz}\right)\mathrm{d}y \\ &\leq \frac{16c_{22}\delta z}{\sqrt{Q_0}} \sum_{j\in\mathbb{Z}} \frac{\hat{\phi}(8j\delta z)}{r^*} \sum_{l\in\mathbb{Z}} \hat{\phi}\left(\frac{2c_{22}l\delta}{r^*\sqrt{Q_0}}\right)\left|\sum_{d=1}^{r^*} e\left(\frac{j^*bd^2+ld}{r^*}\right)\right| |E(j,l)|,\end{aligned}$$

where

$$E(j,l) := \int_{Q_0}^{2Q_0} e\left(jyz - l\cdot\frac{\sqrt{y}}{r^*}\right)\,\mathrm{d}y.$$

Applying Lemmas 8 and 11, we deduce that the right-hand side of (44) is bounded by

$$(45)\qquad \leq \frac{c_{24}\delta z}{\sqrt{Q_0}} \sum_{|j|\leq 1/(8\delta z)} \frac{1}{\sqrt{r^*}} \sum_{|l|\leq r^*\sqrt{Q_0}/(2c_{22}\delta)} |E(j,l)|\,.$$

We have

$$E(0,0) = Q_0.$$

If $j \neq 0$, then

$$|E(j,0)| \leq \frac{1}{|j|z}.$$

If $l \neq 0$, then

$$|E(0,l)| \leq \frac{c_{25}Q_0^{1/2}}{|l|}$$

by Lemma 9 (take into account that $r^* = 1$ if $j = 0$). If $j \neq 0$ and $l \neq 0$, then Lemma 10 yields

$$|E(j,l)| \leq \frac{c_{26}\sqrt{r^*}Q_0^{3/4}}{\sqrt{|l|}}.$$

Therefore, the expression in (45) is bounded by

$$
\begin{aligned}
(46) \quad &\leq c_{27}\delta\left(z\sqrt{Q_0}+\frac{1}{\sqrt{Q_0}}\sum_{1\leq j\leq 1/(8\delta z)}\frac{1}{j\sqrt{r^*}}+z\sum_{1\leq l\leq\sqrt{Q_0}/(2c_{22}\delta)}\frac{1}{l}+\right.\\
&\qquad \left. zQ_0^{1/4}\sum_{1\leq j\leq 1/(8\delta z)}\ \sum_{1\leq l\leq r^*\sqrt{Q_0}/(2c_{22}\delta)}\frac{1}{\sqrt{l}}\right)\\
&\leq c_{28}\left(\delta z\sqrt{Q_0}+\frac{\delta}{\sqrt{Q_0}}\sum_{1\leq j\leq 1/(8\delta z)}\frac{1}{j\sqrt{r^*}}+\delta z\Delta^{-\varepsilon}+\right.\\
&\qquad \left. z\sqrt{\delta}Q_0^{1/2}\sum_{1\leq j\leq 1/(8\delta z)}\sqrt{r^*}\right).
\end{aligned}
$$

Now, we evaluate the sums over j in the last line of (46). By the definition of r^*, we have

$$
\begin{aligned}
(47) \qquad \sum_{1\leq j\leq 1/(8\delta z)}\frac{1}{j\sqrt{r^*}} &= \frac{1}{\sqrt{r}}\sum_{t|r}\sqrt{t}\sum_{\substack{1\,\leq\, j\,\leq\, 1/(8\delta z)\\(r,\,j)\,=\,t}}\frac{1}{j}\\
&\leq \frac{c_{29}\log(2+1/(8\delta z))}{\sqrt{r}}\sum_{t|r}\frac{1}{\sqrt{t}}\\
&\leq c_{30}\Delta^{-\varepsilon}r^{-1/2}
\end{aligned}
$$

and

$$
\begin{aligned}
(48) \qquad \sum_{1\leq j\leq 1/(8\delta z)}\sqrt{r^*} &= \sqrt{r}\sum_{t|r}\frac{1}{\sqrt{t}}\sum_{\substack{1\,\leq\, j\,\leq\, 1/(8\delta z)\\(r,\,j)\,=\,t}}1\\
&\leq \frac{\sqrt{r}}{8\delta z}\sum_{t|r}\frac{1}{t^{3/2}}\\
&\leq \frac{c_{31}\sqrt{r}}{\delta z}.
\end{aligned}
$$

Combining (39), (40), (41), (44), (45), (46), (47) and (48), we obtain

$$
(49) \quad P\left(\frac{b}{r}+z\right)\leq c_{32}\Delta^{-\varepsilon}\left(1+\delta z\sqrt{Q_0}+\delta Q_0^{-1/2}r^{-1/2}+\delta^{-1/2}Q_0^{1/2}\sqrt{r}\right).
$$

Choosing $\delta := Q_0\Delta/z$, we infer the desired estimate from (49) and (20).□

Acknowledgement. This paper was written during postdoctoral stays at the Harish-Chandra Research Institute at Allahabad (India) and the Department of Mathematics and Statistics at Queen's University in Kingston (Canada). The author wishes to thank these institutions for financial support.

References

[1] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer-Verlag, Berlin ect., 1995.

[2] D. Bump, *Automorphic Forms and Representations*, Cambridge Stud. Adv. Math. 55, Cambridge Univ. Press, Cambridge, 1996.

[3] E. Bombieri, *On the large sieve*, Mathematika 12 (1965) 201-225.

[4] B. Crstici, D.S. Mitrinović, J. Sándor, *Handbook of number theory*, Kluwer Academic Publishers Group, Dordrecht, 1996.

[5] P.D.T.A. Elliott, *On inequalities of large sieve type*, Acta Arith. 18 (1971) 405-422.

[6] S.W. Graham, G. Kolesnik, *Van der Corput's method of exponential sums*, Cambridge University Press, Cambridge ect., 1991.

[7] H.L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin-New York, 1971.

[8] H.L. Montgomery, R.C. Vaughan, *The large sieve*, Mathematika 20 (1973) 119-134.

[9] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An introduction to the theory of numbers*, John Wiley & Sons, New York, 1991.

[10] D. Wolke, *On the large sieve with primes*, Acta Math. Acad. Sci. Hungar. 22 (1971/72) 239-247.

[11] L. Zhao, *Large sieve inequality with characters to square moduli*, Acta Arith. 112 (2004) 297-308.